REMARKS

In response to the Office Action mailed on September 1, 2006, Applicant(s) respectfully request(s) reconsideration. Claim(s) 1-41**are** now pending in this Application.

Claims 1, 18, 21 and 38-41 are independent claims and the remaining claims are dependent claims.

In this Amendment, claim(s) 1, 13, 14, 18, 19, 21, 27, 33, 34, 38-41**have** been amended, claim(s) 9, 10, 22, 26 **has/have** been cancelled and claim(s) 42, 43 **have** been added. Applicant(s) believe that the claim(s) as presented are in condition for allowance. A notice to this affect is respectfully requested.

Formalities:

The Office Action cites several minor inconsistencies in the specification and claims. Applicant thanks the Examiner for his observations. The inconsistencies have been herein amended.

Rejection under 35 U.S.C. § 101:

Independent claims 1, 18, 21 and 38-41 have been rejected for nonstatutory subject matter. Accordingly, claims 1, 18, 21 and 38-41 have been herein amended to recite subject matter similar to an **encoded set of processor based instructions on a computer readable medium,** to further clarify the statutory class of applicant's invention. Accordingly, it is respectfully requested that the rejection under 35 U.S.C. § 101 be withdrawn.

Rejection under 35 U.S.C. § 112:

The Office Action rejects claim 13. Claim 13 has been amended to recite avoiding analyzing the access attempt, as disclosed at page 7, lines 20-25, to further clarify.

Claim 14 has been amended to recite that the data security decision is indicative of the propriety of the access attempt, as discussed at page 4, lines 28-31. Claims 33 and 34 have been similarly amended. It is therefore respectfully requested that the rejection of these and dependent claims 15, 16 and 34- 36 be withdrawn.

Rejection under 35 U.S.C. § 103(a) based on Krack, U.S. Patent No. 6,941,369 in view of Balasubramaniyan, "An Architecture for Intrusion Detection using Autonomous Agents":

The Office Action rejects claims 1-41 based on Krack '369 in view of Balasubramaniyan. Applicant respectfully submits that the Krack system is inapplicable to the claimed invention because Krack teaches an intermediate firewall disposed between lightweight agents and a primary firewall for load balancing (performance) reasons, while the present claims employ agents for intrusion detection in a trusted region of the host system, already behind any firewalls that may be present.

Specifically, the office action cites claim 1 as anticipated by Krack '369 because, inter alia, Krack supposedly discloses "intercepting the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway" as recited in claim 1. Therefore, Krack '369 presents an intermediate firewall for allowing lightweight applications (web servers 22a..n) to handle and load-balance web traffic while transacting with host applications between the intermediate firewall 15 and the internal firewall 16, thus establishing a so-called protected zone 30 (col. 5:24-36). Krack, therefore, does not intercept, but rather receives the transmission with the expectation of recreating it behind the firewall at a later time, as discussed at col. 6:39-46. In the claimed interception, the transmission is nonintrusively permitted to continue on to the database for effecting the intended transaction (assuming no corrective action is called for), it is not received and later reconstructed as in Krack.

Such claimed interception is further distinguishable from Krack because it is a prioritized interception, meaning that the claimed interception occurs by establishing a notification in a list PRIOR TO the notification provided to the intended access gateway that ultimately receives the transaction (request). This differs from Krack in that the original intended notification for receiving the database request is not replaced or substituted, but merely inserted in front of, as in one "cutting in line." In the system presented by Krack '369, in contrast, Krack employs servers for traversing the

intermediate firewall with a reconstructed (encrypted) web request (col. 6:39-46), not for intercepting local database access. This differs from the presently claimed invention because such local database access is already behind any in-place firewall and is emanating from a presumably "trusted" user.

Accordingly, claim 1 has been herein amended with the subject matter of claims 9 and 10 to include:

determining an IPC mechanism to be employed by a local client for accessing the DB resource, identifying a common access point for the access paths to the protected resource, access attempts occurring via the identified access point for the identified access paths, establishing an IPC intercept from the common access point employed by database clients for accessing the DB resource, and receiving the access attempt at the local agent via the IPC intercept prior to receipt of the access attempt by the access gateway, to further clarify and distinguish the present claims. Nowhere does Krack show, teach, or disclose, alone or in combination, the claimed prioritized interception for intercepting, not replacing, the database request by receiving the access attempt at the local agent via the IPC intercept prior to receipt of the access attempt by the access gateway, as now recited in amended claim 1.

The Office Action further suggests that Balasubramaniyan teaches the use of agents in an intrusion detection system. The Balasubramaniyan agents differ from the disclosed use of agents because the Balasubramaniyan agents are responsive to the front end communications, i.e. from the UI to the firewall, as shown at Balasubramaniyan, p. 17 Figs.1 and 2. The claimed invention employs local agents responsive to a LOCAL access attempt. The local access attempt is already behind any firewall that may be in place (i.e. from a trusted DBA, maintenance or other local account). Therefore, the claimed local agent is responsive to local communications, not to firewall-directed front end communications.

Further, one of ordinary skill in the art would not look to Balasubramaniyan to modify Krack because Balasubramaniyan promotes the use of AUTONOMOUS agents, or independent processes not responsive to or via delegation from a parent or master process (Balasubramaniyan, sec. 1.4). In contrast, the Krack architecture employs

spawned ACMs 33 and web servers 22 responsive to the host 31 and dispatcher 21, respectively (col. 6, lines 3:11). Accordingly, the Krack approach does not lend itself to autonomous agents as suggested by Balasubramaniyan. Further, the authentication exchange (27a,b) at col. 6, lines 11-23 performs a prevention operation against unauthorized access, not a detection operation for identifying such activity once it occurs. If a would-be intruder spoofed or otherwise satisfied the Krack authentication, successive detection would be eluded.

Therefore, if one were to combine the teachings or Balasubramaniyan with Krack 369, the result would not anticipate amended claim 1 because the Krack authentication 27a,b tunnels around the intermediate firewall 15. The Balasubramaniyan agents monitor and report, but do not authenticate and conditionally allow access based on such authentication. In fact, Balasubramaniyan teaches away from cryptographic techniques because of the performance impact (Balasubramaniyan, p. 19, sec. 4.1.2 : Security). Accordingly, even if one were to force the combination, the result would be inoperable because the teachings of Balasubramaniyan do not support authenticated access control (prevention), but merely detection.

Claim 1 is therefore submitted as allowable because the disclosures of Krack and Balasubramaniyan, do not show, teach or disclose, alone or in combination, the claimed intercepting in a prioritized manner as clarified and distinguished in amended claim 1.

Claim 18 has been rejected also based on Krack in view of Balasubramaniyan. The Office Action suggests that Krack '369 teaches the claimed "indexing a notification list corresponding to the identified local event object." In support of this assertion, the Office Action cites a database retrieval operation. The claimed notification list, however, performs non-intrusive interception of the database access by inserting a notification to the local agent BEFORE the notification to the database for processing the event. This assures the agent of notification of the impending database access prior to actual processing of the access by the database, allowing corrective activity before the access is performed, discussed further in the specification at page 14:7-8. Such access occurs via access to the claimed IPC buffer in kernel main memory while processing events as

part of OS (operating system) operation, not as part of processing a user database as the Office Action suggests.

Accordingly, claim 19, reciting these distinctive features, has been amended into claim 18 such that claim 18 now recites that establishing the interception wrapper further comprises identifying, at least one interprocess communication operation, each of the identified IPC operation corresponding to an event, the event derived from a database (DB) instruction, instantiating a local event object corresponding to the event, the local event object having a notification list indicative of notifications of an object to be made upon an occurrence of the event, and storing, in a first position in the notification list, an indication of the local agent, the first position operable to provide the first notification upon an occurrence of the event, prior to other notifications in the notification list, to further clarify and distinguish claim 18. Accordingly, claim 18 is submitted as allowable because neither Krack nor Balasubramaniyan show, teach, or disclose, alone or in combination, establishment of the interception wrapper as claimed in amended claim 18.

Claim 21 has been rejected based on similar grounds as claim 1. Specifically, the Office Action asserts that Krack teaches intercepting the access attempt. Krack, however, does not teach forwarding the access attempt to a data security device for analysis while preserving the original access for normal processing via the common access point. The claimed data security device operates remotely from the database for analyzing network traffic. The local access attempts intercepted by the local agent are transmitted back out "over the wire" (network connection) to the remote data security device for analysis as any other incoming network DB request (recall that the local agent is directed to LOCAL access attempts, such as DBA accounts, maintenance accounts, etc., that might otherwise have the effect of "bypassing" the front line security of the network based data security device).

Therefore, the claimed agent operates in a distinguishable manner form Krack because it transmits the DB request outbound from the host to a data security device. Krack only addresses inbound firewall-directed DB requests, and does not transmit to a remote data security device from the host from BEHIND the firewall.

Accordingly, claim 21 has been herein amended to recite features of clams 22 and 26 (having subject matter similar to claims 2 and 6) to recite the access attempt being deterministic of a DB instruction, the local agent being in communication with a data security device operable to analyze the propriety of the access attempt from objects and data values referenced by the DB instruction, and further that the local agent [is] further operable to reroute the intercepted access attempts to the data security device, the data security device operable to offload data security decisions as a consolidated appliance, the offloaded data security decisions relieving the host from processing the data security decisions, to further clarify and distinguish claim 21.

Claim 38, rejected on similar grounds as claim 18, has been likewise amended and is therefore believed allowable for the same reasons.

Claim 39, rejected on grounds similar to claim 1, has been likewise amended and is therefore believed allowable for the same reasons.

Claim 40, rejected on similar grounds as claim 21, has been likewise amended and is therefore believed allowable for the same reasons.

Claim 41, rejected on similar grounds as claims 1 and 21, has been herein amended with the subject matter of claims 2, 6, 9 and 10 to further clarify distinguishing features of Applicant's claims.

New claim 42 has been herein added, including subject matter of claims 1, 2, 5, 6, 9 and 10 to further recite distinguishing features of applicant's claimed invention, as discussed above. New claim 43 has also been added to recite subject matter of claim 19, also as discussed above.

As the remaining claims depend, either directly or indirectly, from claims 1, 18 and 21, it is respectfully submitted that all claims now in the case are in condition for allowance.

The Office Action objects to the Drawings. Corrected drawings are enclosed herein.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response,

including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,

Christopher J. Lutz, Esq.
Attorney for Applicant(s)
Registration No.: 44,883
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: GRD03-04

Dated: December 1, 2006